2131
41

Lawrence W. Langley
U.S. Patent Agent, Professional Engineer
2733 Big Falls Road
Blacksburg, VA 24060
H(540) 633-2733 W(540) 961-2001

IN THE UNITED STATES
PATENT AND TRADEMARK OFFICE

IN RE APPLICATION OF

Gail A. Langley **Group Art Unit:**

Serial No. 09,781,607

Examiner: Longbit Chai

Filed: February 1, 2000

For: KEY CARD FOR PERSONAL HOME PAGE ACCESS

September 28, 2004

The Honorable Commissioner of
Patents and Trademarks
Washington, D.C. 20231

RESPONSE TO FIRST OFFICE ACTION

Examiner rejects Claims 1 and 2 under 35 U.S.C. 103(a) as being unpatentable over Scroggie et al (Patent number 6014634), hereinafter referred to as Scroggie, in view of Beuk et al (Patent number 5446266), hereinafter referred to as Beuk.

Scroggie describes a method and apparatus for providing shopping aids and incentives to customers through a computer network. As a part of the method, a prompt for personal information is transmitted from a main retail store computer to a customer's personal computer over the computer network (Scroggie Column 16 Lines 59-61). In response, personal information data is uploaded from the personal computer to the main computer (Scroggie Column 16, Lines 62-65). The prompt is typically the only information transmitted to the personal computer from the main computer.

The purposes served by Scroggie are clearly indicated by the language of claim 14.

"A system for providing purchasing incentives to consumers, comprising::

a main computer having a purchase history database for storing product data for products purchased in association with a unique identifier and a personal page database;

a computer network;

at least one personal computer coupled to said main computer via said computer network;

said main computer configured to transmit a prompt for personal information to said at least one personal computer over said computer network;

said at least one personal computer configured to transmit personal information data from to said main computer over said computer network in response to said prompt;

said main computer configured to generate page data defining a personal web page that is accessible over said computer network, said personal web page based at least in part on said personal information data transmitted from said at least one personal computer to said main computer;

said main computer configured to assign a web page address to said personal web page based upon said personal information data;

said main computer configured to store said page data defining said personal web page in said personal page database;

said main computer configured to determine a purchase incentive depending on (1) said product data stored in said purchase history database or (2) said page data stored in said personal page database; and

said main computer configured to update said page data so that said personal web page will display said purchase incentive."

In contrast, Applicant's invention allows information from a data source such as a grocery store main computer to be transmitted to the customer's home page or personal computer (Applicant's Page 2, Lines 6-13). The information transmitted consists of product data and descriptions desired by the customer. This information is generated as a result of the customer's transaction at the store, and only when the customer requests it. The purpose of the invention is to give the customer secure, private access over the Internet to information relating to his or her own purchases, while preventing access to the customer's home page or computer by unauthorized parties. No personal information data is transmitted from the customer's computer to the store's main computer.

The inventions are opposite in their objectives. Scroggie serves the interests of the store by allowing it to accumulate marketing information about its customer base from customers' computers, while applicant's invention serves the interest of the customer by enabling him or her to obtain information relating to actual purchases from the store computer. Optimally the information transmitted from the store is in a form that facilitates subsequent processing by the customer using a spreadsheet, data base system or word processor. Scroggie contains no indication that the customer is in control of information transmitted from the store computer, except for the usual limitations imposed by normal access to an internet website. The store can sell the customer's IP address or share it with other organizations, potentially subjecting the customer to unsolicited and undesired messages from third parties.

In contrast, applicant's invention authorizes access to a customer's home page or personal computer only when the key card is personally presented at the store by the customer.

Examiner cites Column 17, Lines 4-7 of Scroggie as claiming an authorization code stored in said data base, The language of this claim element is as follows.

"- - assigning a web page address to said personal web page based upon said personal information data, storing said page data defining said personal web page in a personal page database: - - ."

There is no mention here of an authorization code or, indeed, any indication that the information stored in the customer's web page is controlled, limited or constrained by the customer.

Examiner refers to Scroggie Column 16, Lines 62-65, which describes an identity code generated during the registration process.

"transmitting personal information data from said personal computer to said main computer over said computer network in response to said prompt, said personal information including an identity code."

The identity code is produced during the registration process, as described in Scroggie Column 9, Lines 50-61 in the specification. The purpose of registration and creation of the identity code is clearly described in Scroggie Column 9, lines 47-49.

"The primary purpose of the registration is customer identification, with a secondary purpose of demographic analysis."

Applicant's authorization code has an entirely different structure and purpose. It limits access to the customer's web page or personal computer only by authorized sources of data. This is clearly not a customer identification means, it is not generated by the store computer and it cannot be used for demographic analysis.

In the same context Examiner refers to Scroggie Column 6, Line 43, which reads as follows:

"- - the consumer will be required to enter a valid Internet address - - "

This is a constraint on the customer's access to the store's computer, not the access by the store's computer to the customer's home page or personal computer. The entire focus of applicant's invention is to limit access to the customer's home page or personal computer.

Examiner cites Beuk, Column 2, Lines 46-49, as disclosing the storage of applicant's authorization code and data base address in a smart card. This citation describes an option to manually enter a security code should the card contain an invalid security code. Applicant's invention does not contain such an option. The authorization code and data base address are never entered manually. This would defeat one main purpose of applicant's key card, which is to make manual security code entry unnecessary.

Beuk's smart card is directly inserted in Control device C, which contains apparatus to be protected. Beuk does not mention a network connection between the card and the apparatus, and also does not disclose any means for control of information transmitted to a customer's home page or personal computer. Beuk's card is used for local control of an apparatus such as a car, a car radio or a car telephone, not for control of communications over the Internet. The security provisions of Beuk are to prevent unauthorized operation of the apparatus, rather than to prevent unauthorized transmittal of information. In contrast, applicant's invention does not control local operation of an apparatus, but controls remote data storage over the Internet in a personal home page or personal computer.

Examiner cites Beuk, Column 1, Lines 53-56 as disclosing the use of a smart card type of data carrier, optionally containing data representing user-specific apparatus settings. Applicant's key card is not a smart card whose data contents may be modified to represent the settings of different users. It is a card containing fixed information consisting of an authorization code and a network address, not modified for different users, and not capable of being modified manually. Any provision for modification of the card's contents would defeat another main purpose of applicant's invention, which is to make it unnecessary for the customer to remember any authorization code or Internet address information.

Examiner maintains that the combination of Scroggie and Beuk would make applicant's invention obvious to one skilled in the art. How would a system for distributing premiums to customers using the Internet be combined with a local control system for an apparatus using a smart card, to achieve the functions and purpose of applicant's invention? The flow of information in the system for distributing premiums would first have to be reversed, that is, instead of accumulating marketing information about its customer base from customers' computers, the system of Scroggie would have to be modified to deliver information from a data source such as a grocery store main computer to the customer's home page or personal computer. Then the system of Beuk would have to be modified to control an information transmission process on a network, instead of controlling an apparatus locally. Then the combination of the two systems would have to be modified to add the security feature of a key card that contains all the information necessary to establish communication to the customer's home page or personal computer, a card that does not require a manual entry by the customer. The combination of two systems whose purposes are so diametrically opposite to applicant's objectives would require an inventive process, and could not be achieved by the exercise of ordinary engineering.

For the above reasons, applicant respectfully opposes examiner's contention that the combination of Scroggie and Beuk makes the instant invention obvious to a person skilled in the art.

Examiner rejected applicant's Claim 2 on the basis that Scroggie teaches use of the Internet for transmission of data in a system for distributing purchasing incentives. However, the source of data in Scroggie is the customer, while the source of data in applicant's invention is the retail store or other remote data source. The data destination in Scroggie is a data base in the retail store's computer, while the data destination in Applicant's invention is the customer's home page or personal computer. The flow of information is in opposite directions in the two systems. Furthermore, the purpose of the information flow in Scroggie is to serve the interests of the retail store, and to serve the interests of the customer in Applicant's invention. Applicant respectfully objects to the assertion that these systems are equivalent.

Examiner rejects applicant's Claim 3 under 35 U.S.C 103(a) as being unpatentable over Scroggie in view of Beuk and Vu. Vu describes a secure processing environment within a computer for processing cryptographic keys and encrypted information. The environment is produced by defining a secure processing mode during the power-on sequence of the computer, a mode that cannot be interrupted by other software that may be resident in the computer. While this system may improve the security of encryption and decryption of information by a computer that has other functions, it is not applicable to applicant's invention. To require a power-on cycle as a part of each transaction in the retail store's computer or the computer containing the customer's home page, or even the customer's personal computer, would impose an impossible constraint on system operation. The security of conventional public-key encryption is adequate for applicant's system, because the information protected does not have high intrinsic value to outsiders.

On the other hand, the system of Vu could be used during the power-on sequence of any of the said computers, to achieve greater security in processing encrypted information. This possibility does not impact the patentability of applicant's invention because the secure processing mode would precede and not directly influence operation of applicant's invention. Applicant respectfully objects to examiner's rejection of Claim 3, on the basis that the addition of Vu is simply impractical in the one case, and irrelevant in the other.

Examiner rejects applicant's Claim 4 and 5 under 35 U.S.C 103(a) as being unpatentable over Scroggie in view of Beuk, Vu and in view of RSA-PKCS#5

(Password-based Cryptography Standard, Version 2.0, 1999) hereinafter referred to as RSA-PKCS#5. Neither Beuk nor Scroggie mention encryption or passwording as additional security measures to protect encoded information such as Scroggie's retailer identity or Beuk's product code, consumer household ID, offer code, expiration date, serial number, consumer's name and confirmation number. All these items of information are encoded, but not encrypted or passworded. Applicant's invention provides an additional level of security by encrypting the authorization code and network address, using a password, as claimed in Claim 4. A keyboard is only one possible means of password entry.

Applicant believes that the facts in the above discussion overcome the objections raised by the Examiner, and respectfully requests that the application be passed to issue.

Please address all correspondence relating to the above identified application to the undersigned at the address above.

Lawrence W. Langley

Lawrence W. Langley